On local-global divisibility by p^n in elliptic curves

Laura Paladino, Gabriele Ranieri, Evelina Viada*

Abstract

Let p be a prime number and let k be a number field, which does not contain the field $\mathbb{Q}(\zeta_p+\overline{\zeta_p})$. Let $\mathcal{E}$ be an elliptic curve defined over k. We prove that if there are no k-rational torsion points of exact order p on $\mathcal{E}$, then the local-global principle holds for divisibility by p^n, with n a natural number. As a consequence of the deep theorem of Merel, for p larger than a constant depending only on the degree of k, there are no counterexamples to the local-global divisibility principle. Nice and deep works give explicit small constants for elliptic curves defined over a number field of degree at most 5 over $\mathbb{Q}$.

1 Introduction

Let k be a number field and let $\mathcal{A}$ be a commutative algebraic group defined over k. Several papers have been written on the following classical question, known as *Local-Global Divisibility Problem.*

PROBLEM: *Let $P \in \mathcal{A}(k)$. Assume that for all but finitely many valuations $v \in k$, there exists $D_v \in \mathcal{A}(k_v)$ such that $P = qD_v$, where q is a positive integer. Is it possible to conclude that there exists $D \in \mathcal{A}(k)$ such that $P = qD$?*

By Bézout's identity, to get answers for a general integer it is sufficient to solve it for powers p^n of a prime. In the classical case of $\mathcal{A} = \mathbb{G}_m$, the answer

*Supported by the Swiss National Science Foundation SNF

is positive for p odd, and negative for instance for $q = 8$ (and $P = 16$) (see for example [AT], [Tro]).

For general commutative algebraic groups, R. Dvornicich and U. Zannier gave some general cohomological criteria, sufficient to answer the question (see [DZ] and [DZ3]). Using these criteria, they found a number of examples an counterexamples to the local-global principle when $\mathcal{A}$ is an elliptic curve or a torus. Further examples in a torus are given by M. Illengo [Ill]. For an elliptic curve $\mathcal{E}$, the local-global principle holds for divisibility by any prime p. Furthermore, they provide a geometric criterium: if $\mathcal{E}$ does not admit any k-isogeny of degree p, then the local-global principle holds for divisibility by p^n. Theorems of Serre and of Mazur (see [Ser] and [Maz2]) prove that such an isogeny exists only for $p \leq c(k, \mathcal{E})$, where $c(k, \mathcal{E})$ is a constant depending on k and $\mathcal{E}$, and on elliptic curves over $\mathbb{Q}$, for $p \in S_1 = \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$. Thus the local-global principle holds in general for p^n with $p > c(k, \mathcal{E})$ and in elliptic curves over $\mathbb{Q}$ it suffices $p \notin S_1$.

The present work answers to a question of Dvornicich and Zannier: *Can one make the constant depending only on the field k and not on $\mathcal{E}$?* In a first paper [PRV], we give positive answer for the very special case of divisibility by p^2. Here we essentially give a strong geometric criterium: if $\mathcal{E}$ does not admit any k-rational torsion point of exact order p, then the local-global principle holds for divisibility by p^n. In view of the deep Merel theorem we give a general positive answer to the above question. More precisely the constant depends only on the degree of k. In an unpublished work, Oesterlé [Oes] showed that there is no k-torsion of exact order larger than $(3^{[k:\mathbb{Q}]/2} + 1)^2$. This constant is not sharp and the bound is expected to be polynomial in the degree. Sharp bounds are hard. They are known only for fields of small degree.The effective Mazur Theorem [Maz] for elliptic curves over $\mathbb{Q}$ allows us to shrunk the set S_1 to $\widetilde{S}_1 = \{2, 3, 5, 7\}$. The results of Kamienny [Kam], Kenku and Momose [KM] and works of Parent [Par] and [Par2] provide the potential minimal sets $S_2 = S_3 = \{2, 3, 5, 7, 11, 13\}$ for elliptic curves over quadratic and cubic fields. Recent unpublished works

by Kamienny, Stein and Stoll [KSS] and Derickx, Kamienny, Stein and Stoll [DKSS] give the potential minimal sets $S_4 = \{2, 3, 5, 7, 11, 13, 17\}$ and $S_5 = \{2, 3, 5, 7, 11, 13, 17, 19\}$ for elliptic curves over fields of degree 4, respectively 5, over $\mathbb{Q}$. Then, outside these sets the local-global-divisibility principle holds. The minimality of such sets for the local-global problem remains an open question, as only counterexamples for 2^n and 3^n, for all $n \geq 2$ are known ([DZ2], [Pal], [Pal2] and [Pal3]).

Theorem 1. *Let p be a prime number and let n be a positive integer. Let $\mathcal{E}$ be an elliptic curve defined over a number field k, which does not contain the field $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$. Suppose that $\mathcal{E}$ does not admit any k-rational torsion point of exact order p. Then, a point $P \in \mathcal{E}(k)$ is locally divisible by p^n in $\mathcal{E}(k_v)$ for all but finitely many valuations v if and only if P is globally divisible by p^n in $\mathcal{E}(k)$.*

The mentioned cohomological criterium of Dvornicich and Zannier asserts that if the local cohomology of $G_n := \mathrm{Gal}(k(\mathcal{E}[p^n])/k)$ is trivial, then there are no counterexamples (see Definition 1 and Theorem 4). Under the hypotheses of our theorem, we prove that the local cohomology of G_n is trivial. For divisibility by p^2, it happens that the structure of G_2 and consequently of its local cohomology is quite simple. The structure of G_n is however quite intricate. Thus, for the general case we cannot apply a direct approach like in the simpler case of the divisibility by p^2. Using an induction, we show that the groups G_n are generated by diagonal, strictly lower triangular and strictly upper triangular matrices. In addition we detect a special diagonal element in G_n. If there are no k-torsion points of exact order p, the local cohomology of these subgroups or of their commutators is trivial. Thanks to the special diagonal element, we glue together the cohomologies and we conclude that the local cohomology of G_n is trivial, too.

As a nice consequence of the deep theorem of L. Merel we produce a complete positive answer to the question of Dvornicich and Zannier.

Corollary 2. *Let $\mathcal{E}$ be an elliptic curve defined over any number field k. Then, there exists a constant $C([k : \mathbb{Q}])$, depending only on the degree of k,*

such that the local-global principle holds for divisibility by any power p^n of primes $p > C([k:\mathbb{Q}])$. In addition $C([k:\mathbb{Q}]) \leq (3^{[k:\mathbb{Q}]/2}+1)^2$.

Proof. By [Mer], for every number field k, there exists a constant $C_{merel}([k:\mathbb{Q}])$ depending only on the degree of k, such that, for every prime $p > C_{merel}([k:\mathbb{Q}])$, no elliptic curve defined over k has a k-rational torsion point of exact order p.
Let p_0 be the largest prime such that k contains the field $\mathbb{Q}(\zeta_{p_0}+\overline{\zeta_{p_0}})$. Observe that $p_0 \leq 2[k:\mathbb{Q}]+1$. Set

$$C([k:\mathbb{Q}]) = \max\{p_0, C_{merel}([k:\mathbb{Q}])\}.$$

In an unpublished work, Oesterlé [Oes] showed that $C_{merel}([k:\mathbb{Q}]) \leq (3^{[k:\mathbb{Q}]/2}+1)^2$. Then, apply Theorem 1. □

The famous Mazur's Theorem and further explicit versions of Merel's Theorem give:

Corollary 3. *Let*

$C(1) = 7$ *for* $\mathbb{Q}$*;*

$C(2) = 13$ *for quadratic fields;*

$C(3) = 13$ *for cubic fields;*

$C(4) = 17$ *for fields of degree* 4 *over* $\mathbb{Q}$*;*

$C(5) = 19$ *for fields of degree* 5 *over* $\mathbb{Q}$*.*

Let $\mathcal{E}$ be an elliptic curve defined over any number field of degree $d = 1, 2, 3, 4, 5$. Then the local-global principle holds for divisibility by any power p^n of primes $p > C(d)$.

Proof. Let k be a field of degree d over $\mathbb{Q}$. Observe that, for every $p > C(d)$, k does not contain $\mathbb{Q}(\zeta_p+\overline{\zeta_p})$. Then, it suffices to replace the known explicit constant for the previous corollary. By the famous Mazur's Theorem (see [Maz]), no elliptic curve defined over $\mathbb{Q}$ has a rational point of exact prime order larger than 7, then $C(1) = 7$. By Kamienny [Kam], Kenku and

Momose [KM], Parent [Par] and [Par2], no elliptic curve defined over a quadratic or a cubic number field k has a k-rational point of exact prime order larger than 13. Then $C(2) = C(3) = 13$. Further recent works in progress by Kamienny, Stein and Stoll [KSS] and Derickx, Kamienny, Stein and Stoll [DKSS] exclude k-rational point of exact prime order larger than 17, respectively 19, for elliptic curves over number fields of degree 4, respectively 5. So $C(4) = 17$ and $C(5) = 19$. □

Acknowledgments. We deeply thank the referee for nice comments and for pointing out the works of Parent, Derickx, Kamienny, Stein and Stoll which give further explicit applications of our theorem. We would like to kindly thank F. Gillibert for her interesting remarks. The third author thanks the Swiss National Science Foundation for financial support.

2 Preliminary results

Let k be a number field and let $\mathcal{E}$ be an elliptic curve defined over k. Let p be a prime. For every positive integer n, we denote by $\mathcal{E}[p^n]$ the p^n-torsion subgroup of $\mathcal{E}$ and by $K_n = k(\mathcal{E}[p^n])$ the number field obtained by adding to k the coordinates of the p^n-torsion points of $\mathcal{E}$. By the Weil pairing, the field K_n is forced to contain a primitive p^nth root of unity ζ_{p^n} (see for example [Sil, Chapter III, Corollary 8.1.1]). Let $G_n = \mathrm{Gal}(K_n/k)$. As usual, we shall view $\mathcal{E}[p^n]$ as $\mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$ and consequently we shall represent G_n as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$, denoted by the same symbol.

As mentioned, the answer to the *Local-Global Divisibility Problem* for p^n is strictly connected to the vanishing condition of the cohomological group $H^1(G_n, \mathcal{E}[p^n])$ and of the local cohomological group $H^1_{\mathrm{loc}}(G_n, \mathcal{E}[p^n])$. Let us recall definitions and results for $\mathcal{E}$.

Definition 1 (Dvornicich, Zannier [DZ])**.** Let Σ be a group and let M be a Σ-module. We say that a cocycle $[c] = [\{Z_\sigma\}] \in H^1(\Sigma, M)$ satisfies the *local conditions* if there exists $W_\sigma \in M$ such that $Z_\sigma = (\sigma - 1)W_\sigma$, for all $\sigma \in \Sigma$. We denote by $H^1_{\mathrm{loc}}(\Sigma, M)$ the subgroup of $H^1(\Sigma, M)$ formed by

such cocycles. Equivalently, $H^1_{\mathrm{loc}}(\Sigma, M)$ is the intersection of the kernels of the restriction maps $H^1(\Sigma, M) \to H^1(C, M)$ as C varies over all cyclic subgroups of Σ.

Theorem 4 (Dvornicich, Zannier [DZ]). *Assume that $H^1_{\mathrm{loc}}(G_n, \mathcal{E}[p^n]) = 0$. Let $P \in \mathcal{E}(k)$ be a point locally divisible by p^n almost everywhere in the completions k_v of k. Then there exists a point $D \in \mathcal{E}(k)$, such that $P = p^n D$.*

In [DZ3] they prove that this theorem is not invertible. Moreover, the remark just after the main theorem and the first few lines of its proof give an intrinsic version of their main theorem [DZ3].

Theorem 5. *Suppose that $\mathcal{E}$ does not admit any k-rational isogeny of degree p. Then $H^1(G_n, \mathcal{E}[p^n]) = 0$, for every $n \in \mathbb{N}$.*

Clearly, if the global cohomology $H^1(G_n, \mathcal{E}[p^n])$ is trivial then also the local cohomology $H^1_{\mathrm{loc}}(G_n, \mathcal{E}[p^n])$. So by Theorem 4, if $\mathcal{E}$ does not admit any k-rational isogeny of degree p, then the local-global principle holds for p^n.

The following lemma is essentially proved in the proof of the Theorem 5, in [DZ3] beginning of page 29.

Lemma 6. *Suppose that there exists a nontrivial multiple of the identity $\tau \in G_1$. Then $H^1(G_n, \mathcal{E}[p^n]) = 0$, for every $n \in \mathbb{N}$.*

Another remark along their proof concerns the group $G_1 \cap \mathcal{D}$, where $\mathcal{D}$ is the subgroup of diagonal matrices of $\mathrm{GL}_2(\mathbb{F}_p)$.

Corollary 7. *Suppose that $G_1 \cap \mathcal{D}$ is not cyclic. Then $H^1(G_n, \mathcal{E}[p^n]) = 0$, for every $n \in \mathbb{N}$.*

Proof. Since $G_1 \cap \mathcal{D}$ is not cyclic, it contains at least a nontrivial multiple of the identity. Apply Lemma 6. □

3 Structure of the proof of the Main Theorem

If $H^1(G_n, \mathcal{E}[p^n]) = 0$, then also the local cohomology is trivial and, by Theorem 4, no counterexample can occur. Therefore we can assume with no restriction that $H^1(G_n, \mathcal{E}[p^n]) \neq 0$. We first describe the structure of G_1.

Lemma 8 ([PRV] Lemma 7)**.** *Suppose that $H^1(G_n, \mathcal{E}[p^n]) \neq 0$. Then either*

$$G_1 = \langle \rho \rangle \qquad \text{or} \qquad G_1 = \langle \rho, \sigma \rangle,$$

where $\rho = \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ is either the identity or a diagonal matrix with $\lambda_1 \neq \lambda_2 \mod (p)$ and $\sigma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, in a suitable basis of $\mathcal{E}[p]$.

Proof. For $n = 2$, we have proved the statement in [PRV, Lemma 7]. The proof extends straightforward to a general positive integer n. $\square$

Note that the order of ρ divides $p-1$ and the order of σ is p. We also sum up some immediate, but useful remarks. From the above description of G_1 we directly see that if $\lambda_1 = 1$, then there exists a torsion point of exact order p defined over k. Indeed the first element of the chosen basis is fixed by both ρ and σ. In addition, if $G_1 = \langle \rho \rangle$ and $\lambda_2 = 1$, then the corresponding eigenvector is a torsion point of exact order p defined over k. In the following, we can exclude these trivial cases and we denote

$$\rho = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \text{ with } \lambda_1 \neq \lambda_2 \mod (p) \text{ and } \lambda_1 \neq 1.$$

Furthermore, if G_1 is cyclic then we assume that $\lambda_2 \neq 1$.

The proof of Theorem 1 relies on the following:

Proposition 9. *Suppose that $H^1(G_n, \mathcal{E}[p^n]) \neq 0$ and $\rho = \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ has order at least 3. Then we have:*

1. *If $\lambda_1 \neq 1$ and $\lambda_2 \neq 1$, then $H^1_{\mathrm{loc}}(G_n, \mathcal{E}[p^n]) = 0$;*

2. *If G_1 is not cyclic and $\lambda_2 = 1$, then $H^1_{\mathrm{loc}}(G_n, \mathcal{E}[p^n]) = 0$.*

The following sections are dedicated to the proof of this proposition. We conclude its proof in section 5. We now clarify how to deduce Theorem 1 from this proposition. In view of Theorem 4, our main Theorem is implied by:

Theorem 1'. *Suppose k does not contain $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$. Suppose that $\mathcal{E}$ does not admit any k-rational torsion point of exact order p. Then*

$$H^1_{\mathrm{loc}}(G_n, \mathcal{E}[p^n]) = 0.$$

Proof. If $H^1(G_n, \mathcal{E}[p^n]) = 0$, then clearly also the local cohomology is trivial and nothing has to be proven. We may assume $H^1(G_n, \mathcal{E}[p^n]) \neq 0$ and we show $H^1_{\mathrm{loc}}(G_n, \mathcal{E}[p^n]) = 0$ using Proposition 9. Let P_1, P_2 be a basis of $\mathcal{E}[p]$ such that G_1 is like in Lemma 8. First of all we remark that if k does not contain the field $\mathbb{Q}(\zeta_p + \bar{\zeta}_p)$, then the order of ρ is ≥ 3. In fact, in this case, $[k(\zeta_p) : k] \geq 3$. Recall that, by Lemma 8, the order of ρ is the largest integer relatively prime to p that divides $|G_1|$. In addition $[k(\zeta_p) : k] \mid |G_1|$ and $[k(\zeta_p) : k] \mid p - 1$. Thus ρ has order ≥ 3.

Observe that if $\lambda_1 = 1$, then P_1 is fixed by G_1 and therefore P_1 is a torsion point of exact order p defined over k. Moreover, if G_1 is cyclic and $\lambda_2 = 1$, then P_2 is a torsion point of exact order p defined over k. Thus, we can assume $\lambda_1 \neq 1$ and, furthermore, we can assume that if $\lambda_2 = 1$, then G_1 is not cyclic. By Proposition 9, we get $H^1_{\mathrm{loc}}(G_n, \mathcal{E}[p^n]) = 0$. $\square$

4 Description of the groups G_n

We are going to choose a suitable basis of $\mathcal{E}[p^n]$. In such a basis, we decompose G_n by its subgroups of diagonal, strictly upper triangular and strictly lower triangular matrices. The decomposition in such subgroups and eventually their commutators, will simplify the study of the cohomology.

We first define some subgroups of G_n. Set

$$L = \begin{cases} K_1, & \text{if } G_1 = \langle \rho \rangle; \\ K_1^{\langle \sigma \rangle} & \text{if } G_1 = \langle \rho, \sigma \rangle. \end{cases}$$

Since $\langle \sigma \rangle$ is normal in G_1, then L/k is a cyclic Galois extension. Its Galois group is generated by a restriction of ρ to L. For every integer n, let

$$H_n = \mathrm{Gal}(K_n/L).$$

Since L/k is Galois, H_n is a normal subgroup of G_n. Moreover it is a p-group and $[G_n : H_n]$ is relatively prime to p. Thus it is the unique p-Sylow

subgroup of G_n. We also observe that the exponent of H_n divides p^n. In fact it is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ and it is well known that every p-Sylow subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ has exponent p^n. Then

$$G_n = \langle \rho_n, H_n \rangle,$$

where ρ_n is a lift of ρ to G_n. We first study the lifts ρ_n, then we study H_n.

4.1 The lift of ρ

Lemma 10. *Suppose $H^1(G_n, \mathcal{E}[p^n]) \neq 0$ and $\rho \neq I$. For any lift ρ_n of ρ to G_n, there exists a basis Q_1, Q_2 of $\mathcal{E}[p^n]$, such that ρ_n is diagonal in G_n and the restriction ρ_j of ρ_n to G_j is diagonal with respect to $p^{n-j}Q_1, p^{n-j}Q_2$.*

Proof. The proof is by induction. For $n = 1$ it is evident. We assume the claim for $n-1$ and we prove it for n. Let ρ_n be a lift of ρ. Choose a basis R_1, R_2 of $\mathcal{E}[p^n]$, such that $\{pR_1, pR_2\}$ is the basis of $\mathcal{E}[p^{n-1}]$ that diagonalizes the restriction ρ_{n-1} of ρ_n to G_{n-1}. Then

$$\rho_n \equiv \rho_j \mod (p^j)$$

for $1 \leq j \leq n-1$, with ρ_j as desired. The characteristic polynomial $P(x)$ of ρ_n has integral coefficients. In addition $\lambda_{1,n-1}, \lambda_{2,n-1}$ are distinguished roots of $P(x)$ modulo p, indeed by inductive hypothesis $\rho_{n-1} \equiv \rho \mod (p)$. So the first derivate $P'(\lambda_{i,n-1})$ is not congruent to 0 modulo (p). By Hensel's Lemma, $P(x)$ has roots $\lambda_{i,n} = \lambda_{i,n-1} + t_i p^{n-1}$ with $0 \leq t_i \leq p-1$. Thus ρ_n is diagonalizable in the basis of corresponding eigenvectors and a p^{n-j} multiple gives eigenvectors for a lift of ρ to G_j. $\square$

We fix once and for all a basis $\{Q_1, Q_2\}$ of $\mathcal{E}[p^n]$ with the properties of the above lemma. Consequently we fix the basis $\{p^{n-j}Q_1, p^{n-j}Q_2\}$ of $\mathcal{E}[p^j]$, for $1 \leq j \leq n-1$. The order of such a lift of ρ divides $p^{n-1}(p-1)$ and it is divided by the order of ρ. Taking an appropriate p power of this lift, we obtain a diagonal lift ρ_n of ρ such that the order of ρ_n is equal to the order of ρ.

Definition. We denote by

$$\rho_n = \begin{pmatrix} \lambda_{1,n} & 0 \\ 0 & \lambda_{2,n} \end{pmatrix}$$

a diagonal lift of ρ to G_n of the same order than ρ.

Remark 11. Assume that $H^1(G_n, \mathcal{E}[p^n]) \neq 0$ and that ρ has order ≥ 3. Then $\lambda_{2,n}\lambda_{1,n}^{-1} - \lambda_{1,n}\lambda_{2,n}^{-1}$ is invertible (where $\lambda_{i,n}^{-1}$ is the inverse of $\lambda_{i,n}$ in $(\mathbb{Z}/p^n\mathbb{Z})^*$). Indeed, if $\lambda_{2,n}\lambda_{1,n}^{-1} - \lambda_{1,n}\lambda_{2,n}^{-1} \equiv 0 \mod (p)$, then $\lambda_{1,n}^2 \equiv \lambda_{2,n}^2 \mod (p)$. Thus $\lambda_1^2 \equiv \lambda_2^2 \mod (p)$ and ρ^2 is a scalar multiple of the identity. But in view of Corollary 7, only the identity is such a multiple in G_1. Then $\rho^2 = I$, which is a contradiction.

4.2 The decomposition of G_n

We consider the following subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$:
the subgroup $s\mathcal{U}$ of strictly upper triangular matrices;
the subgroup $s\mathcal{L}$ of strictly lower triangular matrices;
the subgroup $\mathcal{D}$ of diagonal matrices.

We decompose $H_n = \mathrm{Gal}(K_n/L)$ in products of diagonal, strictly upper triangular and strictly lower triangular matrices. Then the group G_n has a similar decomposition, as it is generated by ρ_n and H_n.

Proposition 12. *Assume that $H^1(G_n, \mathcal{E}[p^n]) \neq 0$ and that the order of ρ is at least 3. Then, the group H_n is generated by matrices of $\mathcal{D}_n = H_n \cap \mathcal{D}$, $s\mathcal{U}_n = H_n \cap s\mathcal{U}$ and $s\mathcal{L}_n = H_n \cap s\mathcal{L}$.*

The proof of Proposition 12 is done by induction. The structure is technical and we do it along several steps. Recall that H_n restricts to either the identity, or $\langle\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\rangle$ modulo p. Therefore every matrix of H_n has the form

$$\begin{pmatrix} 1+pa & e \\ pc & 1+pd \end{pmatrix},$$

with $e \in \mathbb{Z}/p^n\mathbb{Z}$ and $a, c, d \in \mathbb{Z}/p^{n-1}\mathbb{Z}$. Of course every matrix can be decomposed as product of diagonal, strictly upper triangular and strictly

lower triangular matrices. Here we shall prove that for $\tau \in H_n$ such factors are in H_n as well. So, we shall prove that certain matrices are in H_n. Since H_n is normal in G_n, then for every $\tau \in H_n$, also $\rho_n^i \tau^m \rho_n^{-i} \in H_n$, for every integer i, m. Besides, we recall that H_n has exponent dividing p^n and therefore powers of τ are well defined for classes $m \in \mathbb{Z}/p^n\mathbb{Z}$. Other useful matrices in H_n are constructed in the following:

Property 13. *Assume that $H^1(G_n, \mathcal{E}[p^n]) \neq 0$ and $\rho = \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ has order at least 3. Let $H_n^* = \mathrm{Gal}(K_n/K_{n-1}) \subset H_n$. Suppose that*

$$\tau = \begin{pmatrix} 1+p^{n-1}a & p^{n-1}b \\ p^{n-1}c & 1+p^{n-1}d \end{pmatrix} \in H_n^*,$$

for certain $a, b, c, d \in \mathbb{Z}/p\mathbb{Z}$. Then

$$\begin{pmatrix} 1+p^{n-1}a & 0 \\ 0 & 1+p^{n-1}d \end{pmatrix}, \begin{pmatrix} 1 & p^{n-1}b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ p^{n-1}c & 1 \end{pmatrix} \in H_n^*.$$

Proof. We recall the following property of basic linear algebra. Let V be a vector space and W be a subspace of V. Let ϕ be an automorphism of V such that $\phi(W) = W$. Let $v_1, \ldots, v_m \in V$ be eigenvectors of ϕ for distinct eigenvalues. If $v_1 + \ldots + v_m \in W$, then $v_i \in W$, for all i.

Let V_n be the multiplicative subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ of the matrices congruent to I modulo p^{n-1}. With the scalar multiplication given by taking powers, the group V_n is a $\mathbb{Z}/p\mathbb{Z}$-vector space of dimension 4.

Observe that $H_n^* = \mathrm{Gal}(K_n/K_{n-1})$ is a vector subspace of V_n. The map $\phi_n \colon V_n \to V_n\,;\, \tau \to \rho_n \tau \rho_n^{-1}$ is an automorphism. Since H_n^* is normal in G_n, then $\phi_n(H_n^*) = H_n^*$. By a simple verification we can determine a basis of eigenvectors for ϕ_n. To the eigenvalue 1 correspond the two eigenvectors $\left(\begin{smallmatrix} 1+p^{n-1} & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1+p^{n-1} \end{smallmatrix}\right)$; to the eigenvalue $\lambda_1\lambda_2^{-1}$ corresponds the eigenvector $\left(\begin{smallmatrix} 1 & p^{n-1} \\ 0 & 1 \end{smallmatrix}\right)$; and to the eigenvalue $\lambda_2\lambda_1^{-1}$ corresponds the eigenvector $\left(\begin{smallmatrix} 1 & 0 \\ p^{n-1} & 1 \end{smallmatrix}\right)$. Note that, by Remark 11, the last two eigenvalues are distinct. Applying the above result from linear algebra to V_n, H_n^* and ϕ_n, we obtain the desired result. $\square$

We are now ready to prove a property that represents the inductive step for the wished decomposition of H_n.

Property 14. *Assume that $H^1(G_n, \mathcal{E}[p^n]) \neq 0$ and that $\rho = \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ has order at least 3.*

i. Suppose

$$\tau = \begin{pmatrix} 1+pa & p^{n-1}b \\ p^{n-1}c & 1+pd \end{pmatrix} \in H_n,$$

with $a, d \in \mathbb{Z}/p^{n-1}\mathbb{Z}$ and $b, c \in \mathbb{Z}/p\mathbb{Z}$. Then

$$\begin{pmatrix} 1 & p^{n-1}b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ p^{n-1}c & 1 \end{pmatrix} \in H_n.$$

Consequently, τ decomposes in H_n as

$$\tau = \begin{pmatrix} 1+pa & 0 \\ 0 & 1+pd \end{pmatrix} \begin{pmatrix} 1 & p^{n-1}b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^{n-1}c & 1 \end{pmatrix}.$$

ii. Suppose

$$\tau = \begin{pmatrix} 1+p^{n-1}a & p^{n-1}b \\ pc & 1+p^{n-1}d \end{pmatrix} \in H_n$$

with $a, b, d \in \mathbb{Z}/p\mathbb{Z}$ and $c \in \mathbb{Z}/p^{n-1}\mathbb{Z}$. Then

$$\begin{pmatrix} 1+p^{n-1}a & 0 \\ 0 & 1+p^{n-1}d \end{pmatrix}, \begin{pmatrix} 1 & p^{n-1}b \\ 0 & 1 \end{pmatrix} \in H_n.$$

Consequently, τ decomposes in H_n as

$$\tau = \begin{pmatrix} 1 & 0 \\ pc & 1 \end{pmatrix} \begin{pmatrix} 1+p^{n-1}a & 0 \\ 0 & 1+p^{n-1}d \end{pmatrix} \begin{pmatrix} 1 & p^{n-1}b \\ 0 & 1 \end{pmatrix}.$$

iii. Suppose

$$\tau = \begin{pmatrix} 1+p^{n-1}a & e \\ p^{n-1}c & 1+p^{n-1}d \end{pmatrix} \in H_n,$$

with $e \in \mathbb{Z}/p^n\mathbb{Z}$ and $a, c, d \in \mathbb{Z}/p\mathbb{Z}$. Then

$$\begin{pmatrix} 1+p^{n-1}(a-ec) & 0 \\ 0 & 1+p^{n-1}d \end{pmatrix}, \begin{pmatrix} 1 & -p^{n-1}ed \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ p^{n-1}c & 1 \end{pmatrix} \in H_n.$$

Consequently, τ decomposes in H_n as

$$\tau = \begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1+p^{n-1}(a-ec) & 0 \\ 0 & 1+p^{n-1}d \end{pmatrix} \begin{pmatrix} 1 & -p^{n-1}ed \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^{n-1}c & 1 \end{pmatrix}.$$

Proof. Recall that τ^m is well defined for classes $m \in \mathbb{Z}/p^n\mathbb{Z}$.

Part i. Observe that

$$\tau = \begin{pmatrix} 1+pa & 0 \\ 0 & 1+pd \end{pmatrix} \begin{pmatrix} 1 & p^{n-1}b \\ p^{n-1}c & 1 \end{pmatrix}.$$

We are going to show that the second matrix of the product is in H_n and so must be the other. Since H_n is normal in G_n, the matrix $\rho_n \tau \rho_n^{-1} \tau^{-1} \in H_n$. A tedious but simple computation gives

$$\rho_n \tau \rho_n^{-1} \tau^{-1} = \begin{pmatrix} 1 & p^{n-1}b(\lambda_{1,n}\lambda_{2,n}^{-1} - 1) \\ p^{n-1}c(\lambda_{2,n}\lambda_{1,n}^{-1} - 1) & 1 \end{pmatrix} \in H_n.$$

This matrix is in H_n^*, indeed it reduces to the identity modulo p^{n-1}. Applying Property 13 we get

$$\begin{pmatrix} 1 & p^{n-1}b(\lambda_{1,n}\lambda_{2,n}^{-1} - 1) \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ p^{n-1}c(\lambda_{2,n}\lambda_{1,n}^{-1} - 1) & 1 \end{pmatrix} \in H_n^* \subseteq H_n.$$

By remark 11, we know $\lambda_{1,n} \not\equiv \lambda_{2,n} \mod (p)$. So $(\lambda_{1,n}\lambda_{2,n}^{-1} - 1)$ and $(\lambda_{2,n}\lambda_{1,n}^{-1} - 1)$ are invertible in $\mathbb{Z}/p^n\mathbb{Z}$. Taking the associated inverse power, we obtain

$$\begin{pmatrix} 1 & p^{n-1}b \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ p^{n-1}c & 1 \end{pmatrix} \in H_n^* \subset H_n.$$

Thus τ decomposes in H_n as

$$\tau = \begin{pmatrix} 1+pa & 0 \\ 0 & 1+pd \end{pmatrix} \begin{pmatrix} 1 & p^{n-1}b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^{n-1}c & 1 \end{pmatrix}.$$

Part ii. This proof is similar to the previous one. Observe

$$\tau = \begin{pmatrix} 1 & 0 \\ pc & 1 \end{pmatrix} \begin{pmatrix} 1+p^{n-1}a & p^{n-1}b \\ 0 & 1+p^{n-1}d \end{pmatrix}.$$

By induction, we can prove

$$\tau^{\lambda_{2,n}\lambda_{1,n}^{-1}} = \begin{pmatrix} 1+p^{n-1}a\lambda_{2,n}\lambda_{1,n}^{-1} & p^{n-1}b\lambda_{2,n}\lambda_{1,n}^{-1} \\ pc\lambda_{2,n}\lambda_{1,n}^{-1} & 1+p^{n-1}d\lambda_{2,n}\lambda_{1,n}^{-1} \end{pmatrix}.$$

In addition

$$\rho_n \tau \rho_n^{-1} \tau^{-\lambda_{2,n}\lambda_{1,n}^{-1}} = \begin{pmatrix} 1+p^{n-1}a(1-\lambda_{2,n}\lambda_{1,n}^{-1}) & p^{n-1}b(\lambda_{1,n}\lambda_{2,n}^{-1} - \lambda_{2,n}\lambda_{1,n}^{-1}) \\ 0 & 1+p^{n-1}d(1-\lambda_{2,n}\lambda_{1,n}^{-1}) \end{pmatrix} \in H_n.$$

As this matrix is in H_n and reduces to the identity mod p^{n-1}, it is also in H_n^*. Recall that $\lambda_{1,n}^2 \not\equiv \lambda_{2,n}^2 \mod (p)$. Applying Property 13 and taking appropriated powers, we get

$$\begin{pmatrix} 1+p^{n-1}a & 0 \\ 0 & 1+p^{n-1}d \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & p^{n-1}b \\ 0 & 1 \end{pmatrix} \in H_n^* \subset H_n.$$

Thus τ decomposes in H_n as

$$\tau = \begin{pmatrix} 1 & 0 \\ pc & 1 \end{pmatrix} \begin{pmatrix} 1+p^{n-1}a & 0 \\ 0 & 1+p^{n-1}d \end{pmatrix} \begin{pmatrix} 1 & p^{n-1}b \\ 0 & 1 \end{pmatrix}.$$

Part iii. If $p^{n-1} \mid e$, then $\tau \in H_n^*$ and the assertion follows from Property 13. Therefore we can assume that p^{n-1} does not divide e. We compute $\tau^{\lambda_{2,n}\lambda_{1,n}^{-1}}$ which is an element of H_n. By induction, we get

$$\tau^{\lambda_{2,n}\lambda_{1,n}^{-1}} = \begin{pmatrix} 1+p^{n-1}a'' & e\lambda_{2,n}\lambda_{1,n}^{-1} + p^{n-1}b'' \\ p^{n-1}\lambda_{2,n}\lambda_{1,n}^{-1}c & 1+p^{n-1}d'' \end{pmatrix},$$

with $a'', b'', d'' \in \mathbb{Z}/p\mathbb{Z}$. As H_n is normal and $\lambda_{2,n}\lambda_{1,n}^{-1}$ is invertible, the following matrix is in H_n. We have

$$\gamma_1 = \rho_n \tau \rho_n^{-1} \tau^{-\lambda_{2,n}\lambda_{1,n}^{-1}} = \begin{pmatrix} 1+p^{n-1}a' & e(\lambda_{1,n}\lambda_{2,n}^{-1} - \lambda_{2,n}\lambda_{1,n}^{-1}) + p^{n-1}b' \\ 0 & 1+p^{n-1}d' \end{pmatrix} \in H_n,$$

where $a', b', d' \in \mathbb{Z}/p\mathbb{Z}$. As H_n is normal, also the following matrix is an element of H_n:

$$\gamma_2 = \rho_n \gamma_1 \rho_n^{-1} \gamma_1^{-1} = \begin{pmatrix} 1 & e(\lambda_{1,n}\lambda_{2,n}^{-1} - \lambda_{2,n}\lambda_{1,n}^{-1})(\lambda_{1,n}\lambda_{2,n}^{-1} - 1) + p^{n-1}e' \\ 0 & 1 \end{pmatrix},$$

where $e' \in \mathbb{Z}/p\mathbb{Z}$. Recall that $l = (\lambda_{1,n}\lambda_{2,n}^{-1} - \lambda_{2,n}\lambda_{1,n}^{-1})(\lambda_{1,n}\lambda_{2,n}^{-1} - 1)$ is invertible and that p^{n-1} does not divide e. So $e = p^r f$ with f coprime to p and $r < n-1$. Then $\lambda = l + p^{n-r-1}e'f^{-1}$ is invertible in $\mathbb{Z}/p^n\mathbb{Z}$ and $\gamma_2^{\lambda^{-1}} = \left(\begin{smallmatrix} 1 & e \\ 0 & 1 \end{smallmatrix}\right)$. Thus $\left(\begin{smallmatrix} 1 & e \\ 0 & 1 \end{smallmatrix}\right)$ is in H_n. A simple computation gives

$$\tau = \begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1+p^{n-1}(a-ec) & -p^{n-1}ed \\ p^{n-1}c & 1+p^{n-1}d \end{pmatrix}.$$

The second matrix is in H_n^*. By Property 13, the matrices $\left(\begin{smallmatrix} 1+p^{n-1}(a-ec) & 0 \\ 0 & 1+p^{n-1}d \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & -p^{n-1}ed \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ p^{n-1}c & 1 \end{smallmatrix}\right)$ are in H_n^* and consequently in H_n. Thus τ decomposes

in H_n as

$$\tau = \begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 + p^{n-1}(a - ec) & 0 \\ 0 & 1 + p^{n-1}d \end{pmatrix} \begin{pmatrix} 1 & -p^{n-1}ed \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^{n-1}c & 1 \end{pmatrix}.$$

□

The above property is exactly the inductive step to decompose H_n as product of diagonal, strictly upper triangular and strictly lower triangular matrices.

Proof of Proposition 12. Proceed by induction. For H_1, which is either the identity or $\langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle$, the claim is clear. Suppose that H_r is decomposable as product of such matrices for $r < n$. We show it for n. Let τ be a matrix in H_n. Then the reduction τ_{n-1} of τ mod p^{n-1} is a product $\prod \delta_i$ of diagonal, strictly upper triangular and strictly lower triangular matrices. Consider lifts $\tilde{\delta}_i$ of δ_i to H_n. Then $\tau = \tilde{\delta} \prod \tilde{\delta}_i$, where $\tilde{\delta}$ reduced to the identity mod p^{n-1}. Therefore it is sufficient to prove the assertion for a matrix reducing to a diagonal, to a strictly upper triangular or to a strictly lower triangular matrix mod p^{n-1}. By Property 14, the matrix τ can be decomposed in the desired product. □

4.3 Some commutators

To study the cohomology we still need to describe the commutators of some of the subgroups of G_n. We denote by $\mathcal{U}$ the subgroup of upper triangular matrices of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ and by $\mathcal{L}$ the subgroup of lower triangular matrices of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$.

Lemma 15. *The commutators $\mathcal{U}_n'$ and $\mathcal{L}_n'$ of the groups $\mathcal{U}_n = G_n \cap \mathcal{U}$ and $\mathcal{L}_n = G_n \cap \mathcal{L}$ in G_n are cyclic. If in addition $H^1(G_n, \mathcal{E}[p^n]) \neq 0$, the order of ρ is at least* 3 *and G_1 is not cyclic, then*

$$\mathcal{U}_n' = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

Proof. The commutator subgroup $\mathcal{U}_n'$ is generated by the elements $\delta\gamma\delta^{-1}\gamma^{-1}$, with

$$\delta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \gamma = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \in \mathcal{U}_n,$$

where the entries are in $\mathbb{Z}/p^n\mathbb{Z}$ and the elements on the diagonals are invertible modulo p^n. A short computation shows that

$$\delta\gamma\delta^{-1}\gamma^{-1} = \begin{pmatrix} 1 & (ab' - a'b + bd' - b'd)d^{-1}d'^{-1} \\ 0 & 1 \end{pmatrix}. \tag{4.1}$$

Then

$$\mathcal{U}_n' = \left\langle \begin{pmatrix} 1 & p^j \\ 0 & 1 \end{pmatrix} \right\rangle,$$

for an integer $j \in \mathbb{N}$. The proof for $\mathcal{L}_n'$ is analogous.

Suppose that in addition $H^1(G_n, \mathcal{E}[p^n]) \neq 0$, the order of ρ is at least 3 and G_1 is not cyclic. Then $\sigma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in G_1$. Let σ_n be a lift of σ to G_n. By Proposition 12, σ_n decomposes as a product of diagonal, strictly upper triangular and strictly lower triangular matrices. Since σ_n does not restrict to a diagonal matrix, at least one of its factors is of the type

$$\delta = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad \text{with} \quad b \not\equiv 0 \mod (p).$$

A simple computation gives

$$\rho_n\delta\rho_n^{-1}\delta^{-1} = \begin{pmatrix} 1 & (\lambda_{1,n}\lambda_{2,n}^{-1} - 1)b \\ 0 & 1 \end{pmatrix} \in \mathcal{U}_n'.$$

Recall that $\lambda_{1,n} \not\equiv \lambda_{2,n} \mod (p)$ and $b \not\equiv 0 \mod (p)$. Then a power of this matrix is $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \mathcal{U}_n'$.

□

5 Proof of Proposition 8

In this section we study the cohomology of G_n. We recall a useful classical lemma.

Lemma 16 (Sah Theorem, [Lan] Theorem 5.1). *Let Σ be a group and let M be a Σ-module. Let α be in the center of Σ. Then $H^1(\Sigma, M)$ is annihilated by the map $x \to \alpha x - x$ on M. In particular, if this map is an automorphism of M, then $H^1(\Sigma, M) = 0$.*

In the following proposition, we study the relation between the eigenvalues of $\rho = \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ and the triviality of the local cohomology of certain subgroups of G_n. Such subgroups have intersections that allows us to glue those cohomologies together and to deduce the triviality of the local cohomology of G_n.

Proposition 17. *Assume that $H^1(G_n, \mathcal{E}[p^n]) \neq 0$ and that $\rho = \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ has order at least 3. Then, we have:*

1. *The groups $H^1_{\mathrm{loc}}(\langle \rho_n, s\mathcal{U}_n \rangle, \mathcal{E}[p^n])$ and $H^1_{\mathrm{loc}}(\langle \rho_n, s\mathcal{L}_n \rangle, \mathcal{E}[p^n])$ are trivial;*
2. *If $\lambda_1 \neq 1$ and $\lambda_2 \neq 1$, then $H^1_{\mathrm{loc}}(\mathcal{U}_n, \mathcal{E}[p^n])$ and $H^1_{\mathrm{loc}}(\mathcal{L}_n, \mathcal{E}[p^n])$ are trivial;*
3. *If G_1 is not cyclic and $\lambda_2 = 1$, then $H^1_{\mathrm{loc}}(\mathcal{U}_n, \mathcal{E}[p^n]) = 0$.*

Proof. Part 1. We prove the triviality of $H^1_{\mathrm{loc}}(\langle \rho_n, s\mathcal{L}_n \rangle, \mathcal{E}[p^n])$. The triviality of $H^1_{\mathrm{loc}}(\langle \rho_n, s\mathcal{U}_n \rangle, \mathcal{E}[p^n])$ is similar and it is left to the reader.

Remark that $s\mathcal{L}_n$ is cyclic generated by $\left(\begin{smallmatrix} 1 & 0 \\ p^j & 1 \end{smallmatrix}\right)$ where p^j is the minimal power of p dividing all the entries c of any matrix $\left(\begin{smallmatrix} 1 & 0 \\ c & 1 \end{smallmatrix}\right) \in G_n$. Then, we immediately get $H^1_{\mathrm{loc}}(s\mathcal{L}_n, \mathcal{E}[p^n]) = 0$. Moreover $s\mathcal{L}_n$ is a normal subgroup of $\langle \rho_n, s\mathcal{L}_n \rangle$. The order of ρ_n is equal to the order of ρ, which is relatively prime to p. Thus $s\mathcal{L}_n$ is the p-Sylow subgroup of $\langle \rho_n, s\mathcal{L}_n \rangle$. By [DZ, Proposition 2.5], if $H^1_{\mathrm{loc}}(s\mathcal{L}_n, \mathcal{E}[p^n]) = 0$ then $H^1_{\mathrm{loc}}(\langle \rho_n, s\mathcal{L}_n \rangle, \mathcal{E}[p^n]) = 0$.

Part 2. We only present the proof for $\mathcal{U}_n$. The proof for $\mathcal{L}_n$ is similar. Since $\mathcal{U}'_n$ is normal, we have the inflaction-restriction sequence:

$$0 \to H^1(\mathcal{U}_n/\mathcal{U}'_n, \mathcal{E}[p^n]^{\mathcal{U}'_n}) \to H^1(\mathcal{U}_n, \mathcal{E}[p^n]) \to H^1(\mathcal{U}'_n, \mathcal{E}[p^n]).$$

The matrix $\rho_n \in \mathcal{U}_n$ is diagonal and modulo p reduces to ρ. By hypothesis, the eigenvalues λ_1, λ_2 of ρ are both different from 1. Thus $\rho_n - I$ is an

isomorphism of $\mathcal{E}[p^n]$ to itself. Let $[\rho_n]$ be the class of ρ_n in $\mathcal{U}_n/\mathcal{U}'_n$. Then $[\rho_n] - I$ is an isomorphism of $\mathcal{E}[p^n]^{\mathcal{U}'_n}$ into itself. Since $\mathcal{U}_n/\mathcal{U}'_n$ is abelian, then by Lemma 16

$$H^1(\mathcal{U}_n/\mathcal{U}'_n, \mathcal{E}[p^n]^{\mathcal{U}'_n}) = 0. \tag{5.1}$$

On the other hand, by Lemma 15, $\mathcal{U}'_n$ is cyclic. Moreover $H^1_{\text{loc}}(\mathcal{U}_n, \mathcal{E}[p^n])$ is the intersection of the kernels of the restriction maps $H^1(\mathcal{U}_n, \mathcal{E}[p^n]) \to H^1(C, \mathcal{E}[p^n])$, as C varies over all cyclic subgroups of $\mathcal{U}_n$ (see Definition 1). If $H^1_{\text{loc}}(\mathcal{U}_n, \mathcal{E}[p^n]) \neq 0$, then $H^1(\mathcal{U}_n/\mathcal{U}'_n, \mathcal{E}[p^n]^{\mathcal{U}'_n}) \neq 0$, which contradicts (5.1). So $H^1_{\text{loc}}(\mathcal{U}_n, \mathcal{E}[p^n]) = 0$.

Part 3. As $\mathcal{U}'_n$ is normal in $\mathcal{U}_n$, we consider the inflaction-restriction sequence

$$0 \to H^1(\mathcal{U}_n/\mathcal{U}'_n, \mathcal{E}[p^n]^{\mathcal{U}'_n}) \to H^1(\mathcal{U}_n, \mathcal{E}[p^n]) \to H^1(\mathcal{U}'_n, \mathcal{E}[p^n]).$$

Recall that Q_1 and Q_2 is the basis of $\mathcal{E}[p^n]$ such that $\rho_n = \begin{pmatrix} \lambda_{1,n} & 0 \\ 0 & \lambda_{2,n} \end{pmatrix}$. Then $\rho_n(Q_1) = \lambda_{1,n} Q_1$ and $\rho_n(Q_2) = \lambda_{2,n} Q_2$. We first prove that $\mathcal{E}[p^n]^{\mathcal{U}'_n} \subseteq \langle Q_1 \rangle$. Let $a, b \in \mathbb{Z}/p^n\mathbb{Z}$ and let $aQ_1 + bQ_2 \in \mathcal{E}[p^n]^{\mathcal{U}'_n}$. By Lemma 15, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathcal{U}'_n$. Then

$$aQ_1 + bQ_2 = \sigma_n(aQ_1 + bQ_2) = (a+b)Q_1 + bQ_2.$$

Thus $bQ_1 = 0$. Whence $b = 0$, because Q_1 has exact order p^n.

Let $[\rho_n]$ be the class of ρ_n in $\mathcal{U}_n/\mathcal{U}'_n$. Since ρ has order at least 3 and $\lambda_2 = 1$, then $\lambda_1 \neq 1$. Thus $(\rho_n - I)Q_1 = (\lambda_{1,n} - 1)Q_1$ with $\lambda_{1,n} \not\equiv 1 \mod (p)$. Consequently the restriction of $\rho_n - I$ to $\langle Q_1 \rangle$ is an isomorphism. As $\mathcal{E}[p^n]^{\mathcal{U}'_n} \subseteq \langle Q_1 \rangle$, also $[\rho_n] - I$ is an isomorphism of $\mathcal{E}[p^n]^{\mathcal{U}'_n}$ to itself. Moreover $\mathcal{U}_n/\mathcal{U}'_n$ is abelian. By Lemma 16,

$$H^1(\mathcal{U}_n/\mathcal{U}'_n, \mathcal{E}[p^n]^{\mathcal{U}'_n}) = 0. \tag{5.2}$$

On the other hand, $\mathcal{U}'_n$ is cyclic and $H^1_{\text{loc}}(\mathcal{U}_n, \mathcal{E}[p^n])$ is the intersection of the kernels of the restriction maps $H^1(\mathcal{U}_n, \mathcal{E}[p^n]) \to H^1(C, \mathcal{E}[p^n])$, as C varies over all cyclic subgroups of $\mathcal{U}_n$ (see Definition 1). If $H^1_{\text{loc}}(\mathcal{U}_n, \mathcal{E}[p^n]) \neq 0$, then $H^1(\mathcal{U}_n/\mathcal{U}'_n, \mathcal{E}[p^n]^{\mathcal{U}'_n}) \neq 0$. This contradicts (5.2). So $H^1_{\text{loc}}(\mathcal{U}_n, \mathcal{E}[p^n]) = 0$.

□

We are now ready to conclude the proof of Proposition 9. The core idea is to glue the cohomology of the subgroups of G_n via some special elements in their intersections. In the previous part we already proved that the local cohomology of such subgroups is trivial and so also the local cohomology of G_n is trivial. For the convenience of the reader, we recall the statement:

Proposition 9. *Suppose that $H^1(G_n, \mathcal{E}[p^n]) \neq 0$ and that $\rho = \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ has order at least* 3*.*

1. *If $\lambda_1 \neq 1$ and $\lambda_2 \neq 1$, then $H^1_{\mathrm{loc}}(G_n, \mathcal{E}[p^n]) = 0$;*

2. *If G_1 is not cyclic and $\lambda_2 = 1$, then $H^1_{\mathrm{loc}}(G_n, \mathcal{E}[p^n]) = 0$.*

Proof. Part 1. Consider the restrictions

$$r_L : H^1(G_n, \mathcal{E}[p^n]) \to H^1(\mathcal{L}_n, \mathcal{E}[p^n]),$$

$$r_U : H^1(G_n, \mathcal{E}[p^n]) \to H^1(\mathcal{U}_n, \mathcal{E}[p^n]).$$

Let Z be a cocycle from G_n to $\mathcal{E}[p^n]$, such that its class $[Z] \in H^1_{\mathrm{loc}}(G_n, \mathcal{E}[p^n])$. If a cocycle satisfies the local conditions relative to G_n (see Definition 1), then it satisfies them relative to any subgroup of G_n. Thus $r_L([Z]) \in H^1_{\mathrm{loc}}(\mathcal{L}_n, \mathcal{E}[p^n])$ and $r_U([Z]) \in H^1_{\mathrm{loc}}(\mathcal{U}_n, \mathcal{E}[p^n])$. By Proposition 17 part 2. both local cohomologies are trivial. Therefore $[Z] \in \ker(r_L) \cap \ker(r_U)$. In other words the restriction of Z to $\mathcal{L}_n$ and its restriction to $\mathcal{U}_n$ are coboundaries. Hence, there exist $P, Q \in \mathcal{E}[p^n]$, such that

$$\begin{aligned} Z_\gamma &= \gamma(P) - P \quad \text{for} \quad \text{every} \quad \gamma \in \mathcal{L}_n; \\ Z_\delta &= \delta(Q) - Q \quad \text{for} \quad \text{every} \quad \delta \in \mathcal{U}_n. \end{aligned} \tag{5.3}$$

Observe that $\rho_n \in \mathcal{L}_n \cap \mathcal{U}_n$. Then

$$Z_{\rho_n} = \rho_n(P) - P = \rho_n(Q) - Q.$$

Thus $P - Q \in \ker(\rho_n - I)$. Modulo p, the eigenvalues of ρ_n coincide with λ_1 and λ_2. Therefore $\rho_n - I$ is an isomorphism. In particular $\ker(\rho_n - I) = 0$, which implies $P = Q$. Then $[Z]$ is 0 over the group generated by $\mathcal{L}_n$ and $\mathcal{U}_n$. As G_n is generated by ρ_n and H_n, Proposition 12 implies that G_n is generated by $\mathcal{L}_n$ and $\mathcal{U}_n$. Thus $[Z]$ is 0 over G_n.

Part 2. Consider the restrictions

$$r_{SL} : H^1(G_n, \mathcal{E}[p^n]) \to H^1(\langle \rho_n, s\mathcal{L}_n \rangle, \mathcal{E}[p^n]),$$
$$r_U : H^1(G_n, \mathcal{E}[p^n]) \to H^1(\mathcal{U}_n, \mathcal{E}[p^n]).$$

Let Z be a cocycle from G_n to $\mathcal{E}[p^n]$, such that its class $[Z] \in H^1_{\text{loc}}(G_n, \mathcal{E}[p^n])$. Then $r_{SL}([Z]) \in H^1_{\text{loc}}(\langle \rho_n, s\mathcal{L}_n \rangle, \mathcal{E}[p^n])$ and $r_U([Z]) \in H^1_{\text{loc}}(\mathcal{U}_n, \mathcal{E}[p^n])$, which are trivial by Proposition 17. It follows $[Z] \in \ker(r_{SL}) \cap \ker(r_U)$. Hence, there exist $P, Q \in \mathcal{E}[p^n]$, such that

$$\begin{aligned} Z_\gamma &= \gamma(P) - P \quad \text{for} \quad \text{every} \quad \gamma \in \langle \rho_n, s\mathcal{L}_n \rangle; \\ Z_\delta &= \delta(Q) - Q \quad \text{for} \quad \text{every} \quad \delta \in \mathcal{U}_n. \end{aligned} \tag{5.4}$$

Recall that $\rho_n \in \langle \rho_n, s\mathcal{L}_n \rangle \cap \mathcal{U}_n$. Then

$$Z_{\rho_n} = \rho_n(P) - P = \rho_n(Q) - Q \tag{5.5}$$

and $P - Q \in \ker(\rho_n - I)$. Observe that ρ_n has the same order of ρ and $\lambda_2 = 1$. Since the order of ρ divides $p-1$, and $\lambda_{2,n} \equiv \lambda_2 \pmod p$, then $\lambda_{2,n} = 1$ too. We have $\rho_n - I = \begin{pmatrix} \lambda_{1,n} - 1 & 0 \\ 0 & 0 \end{pmatrix}$, with $\lambda_{1,n} \not\equiv 1 \mod (p)$, because ρ has order at least 3 and $\lambda_2 = 1$. We deduce $P - Q = (0, b)$ for a certain $b \in \mathbb{Z}/p^n\mathbb{Z}$. In addition, $\langle \rho_n, s\mathcal{L}_n \rangle$ is generated by ρ_n and $\tau = \left(\begin{smallmatrix} 1 & 0 \\ p^j & 1 \end{smallmatrix}\right)$. By (5.4), we know $Z_\tau = \tau(P) - P$. But $\tau - I = \begin{pmatrix} 0 & 0 \\ p^j & 0 \end{pmatrix}$. Then $\tau(P) - P = \tau(P - (0, b)) - (P - (0, b)) = \tau(Q) - Q$. Thus

$$Z_\tau = \tau(Q) - Q. \tag{5.6}$$

The group G_n is generated by ρ_n and H_n. In view of Proposition 12, the group G_n is generated by $s\mathcal{L}_n = \langle \tau \rangle$ and $\mathcal{U}_n$. By (5.3), (5.5) and (5.6) we see that Z is a coboundary and so $[Z] = 0$. □

References

[AT] Artin E., Tate J., *Class field theory*, Benjamin, Reading, MA, 1967.

[DKSS] Derickx M., Kamienny S., Stein W., Stoll M., *Torsion points on elliptic curves over number fields of degree* 5, work in progress.

[DZ] Dvornicich R., Zannier U., *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France, **129** (2001), 317-338.

[DZ2] Dvornicich R., Zannier U., *An analogue for elliptic curves of the Grunwald-Wang example*, C. R. Acad. Sci. Paris, Ser. I **338** (2004), 47-50.

[DZ3] Dvornicich R., Zannier U., *On local-global principle for the divisibility of a rational point by a positive integer*, Bull. Lon. Math. Soc., no. **39** (2007), 27-34.

[Kam] Kamienny, S., *Torsion points of elliptic curves and q-coefficients of modular forms*, Invent. Math., no. **109**, (1992), 221-229.

[KSS] Kamienny S., Stein W., Stoll M., *Torsion points on elliptic curves over quartic number fields*, preprint 2011.

[KM] Kenku M. A., Momose F., *Torsion points of elliptic curves defined over quadratic fields*, Nagoya Math. J., no. **109**, (1998), 125-149.

[Ill] Illengo M., *Cohomology of integer matrices and local-global divisibility on the torus*, Le Journal de Théorie des Nombres de Bordeaux, no. **20** (2008), 327-334.

[Lan] Lang S., *Elliptic curves: diophantine analysis*, Grundlehren der Mathemathischen Wissenschaften 231, Springer, 1978.

[Maz] Mazur B., *Modular curves and the Eisenstein Ideal*, Publ. Math., Inst. Hauter Etud. Sci , no. **47**, (1977), 33-186.

[Maz2] Mazur B., *Rational isogenies of prime degree (with an appendix of D. Goldfeld)*, Invent. Math., no. **44**, (1978), 129-162.

[Mer] Merel L., *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124**, (1996), 437-449.

[Oes] Oesterlé J., *Torsion des courbes elliptiques sur les corps de nombres*, preprint.

[Pal] PALADINO L., *Local-global divisibility by* 4 *in elliptic curves defined over* $\mathbb{Q}$, Annali di Matematica Pura e Applicata, no. **189.1**, (2010), 17-23.

[Pal2] PALADINO L., *Elliptic curves with* $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ *and counterexamples to local-global divisibility by 9*, Le Journal de Théorie des Nombres de Bordeaux, Vol. **22**, n. 1 (2010), 138-160.

[Pal3] PALADINO L., *On counterexamples to local-global divisibility in commutative algebraic groups*, Acta Arithmetica, **148** no. 1, (2011), 21-29.

[PRV] PALADINO L., RANIERI G., VIADA E., *Local-Global Divisibility by* p^2 *in elliptic curves*, preprint.

[Par] PARENT P., *Torsion des courbes elliptiques sur les corps cubiques*, Ann. Inst. Fourier no. **50** (3), (2000) 723-749.

[Par2] PARENT P., *No 17-torsion on elliptic curves over cubic number fields*, Journal des Théorie des nombres de Bordeaux no. **15**, (2003) 831-838.

[Ser] SERRE J-P., *Proprietés Galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. no. **15**, (1972) 259-331.

[Sil] SILVERMAN J. H., *The arithmetic of elliptic curves, 2nd edition*, Springer, Heidelberg, 2009.

[Tro] TROST E., *Zur theorie des Potenzreste*, Nieuw Archief voor Wiskunde, no. **18** (2) (1948), 58-61.

Laura Paladino
Dipartimento di Matematica
Università della Calabria
via Ponte Pietro Bucci, cubo 31b
IT-87036 Arcavacata di Rende (CS)
e-mail address: paladino@mat.unical.it

Gabriele Ranieri
Collegio Puteano
Scuola Normale Superiore
Piazza dei Cavalieri 3,
IT-56100 Pisa,
Italy
e-mail address: gabriele.ranieri@sns.it

Evelina Viada
Departement Mathematik
Universität Basel
Rheinsprung, 21
CH-4051 Basel
e-mail address: evelina.viada@unibas.ch

Errata corrige

Laura Paladino, Gabriele Ranieri, Evelina Viada*

Abstract

We correct an inaccuracy in Theorem 5 (which also appears as Theorem 4 in [PRV]), by adding in the statement of this theorem the necessary hypothesis that the number field k does not contain $\mathbb{Q}(\zeta_p + \overline{\zeta}_p)$.

1 Remark

Let p be a prime number, let k be a number field and let $\mathcal{E}$ be an elliptic curve defined over k. For every positive integer n, let $\mathcal{E}[p^n]$ be the p^n-torsion subgroup of $\mathcal{E}$. We denote by K_n the number field generated over k by the coordinates of the elements of $\mathcal{E}[p^n]$. Finally, let G_n be the Galois group $\mathrm{Gal}(K_n/k)$.

In [DZ, Theorem 1], the authors prove that if $k \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$, and $\mathcal{E}$ does not admit any k-isogeny of degree p, then $H_1(G_n, E[p^n]) = 0$, for every positive integer n. We shall sligtly extend this result, and substitute Theorem 5 and [PRV, Theorem 4] with the following theorem, which proof follows the one of [DZ]. This does not have any consequences on the results in this article and in [PRV], as we always assume that k does not contain $\mathbb{Q}(\zeta_p + \overline{\zeta_p})$.

Theorem 1. *Let p be a prime number, let k be a number field not containing $\mathbb{Q}(\zeta_p+\overline{\zeta}_p)$ and let $\mathcal{E}$ be an elliptic curve defined over k. Suppose that $\mathcal{E}$ does*

*supported by the Fond National Suisse

not admit any k-isogeny of degree p. Then $H^1(G_n, \mathcal{E}[p^n]) = 0$, for every positive integer n.

Proof. We recall that K_1 contains a primitive pth root of unity ζ_p and $\tau(\zeta_p) = \zeta_p^{\det(\tau)}$ for $\tau \in G_1$. Then $k(\zeta_p) = K_1^{\ker(\det)}$. Since $k \not\supset \mathbb{Q}(\zeta_p + \overline{\zeta}_p)$ and $\mathrm{Gal}(k(\zeta_p)/k)$ is isomorphic to a subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$, then $\mathrm{Gal}(k(\zeta_p)/k)$ is a cyclic group with order $d > 2$ dividing $p-1$. Following line by line the proof of Dvornicich and Zannier in [DZ, Theorem 1], we get that the natural map $G_1 \to \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is injective. Moreover, G_1 is either contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, or it is cyclic, or it is dihedral, or it is an exceptional subgroup (i.e. it is isomorphic to A_4, to S_4 or to A_5, see also [Ser, Proposition 16]).

If G_1 is contained in a Borel subgroup, then G_1 stabilizes a subgroup of order p of $\mathcal{E}[p]$. This contradicts the non existence of an isogeny of degree p defined over k.

Following line by line the last part of the proof of Dvornicich and Zannier, see [DZ, pp. 29-30], by using the fact that $d > 2$, we get that G_1 is not cyclic.

Suppose that G_1 is dihedral. Then G_1 is generated by elements of order 2. Thus $G_1/\ker(\det) \cong \mathrm{Gal}(k(\zeta_p)/k)$ has order ≤ 2, contradicting $d > 2$.

Finally suppose that G_1 is isomorphic to A_4, to S_4 or to A_5. Each these groups have a subgroup R isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Since 2 divides $p-1$ and R is abelian, then the elements of R are simultaneously diagonalizable in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Moreover, the subgroup of the diagonal matrices of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ has exactly three distinct elements of order 2 and among them is $-I$. Then $-I \in R \subset G_1$ contradicts the injectivity of the map $G_1 \to \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$. □

References

[DZ] Dvornicich R., Zannier U., *On local-global principle for the divisibility of a rational point by a positive integer*, Bull. Lon. Math. Soc., no. **39** (2007), 27-34.

[PRV] Paladino L., Ranieri G., Viada E., *Local-Global Divisibility by p^n in elliptic curves*, Bull. London Math. Soc., no. **44** (2012), 789-802.

[Ser] SERRE J-P., *Proprietés Galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math., no. **15**, (1972) 259-331.

Laura Paladino
Dipartimento di Matematica
Università della Calabria
via Ponte Pietro Bucci, cubo 31b
IT-87036 Arcavacata di Rende (CS)
e-mail address: paladino@mat.unical.it

Gabriele Ranieri
Collegio Puteano
Scuola Normale Superiore
Piazza dei Cavalieri 3,
IT-56100 Pisa,
Italy
e-mail address: gabriele.ranieri@sns.it

Evelina Viada
Departement Mathematik
Universität Basel
Rheinsprung, 21
CH-4051 Basel
e-mail address: evelina.viada@unibas.ch